Structuring Defence Cyber-Survivability T&E to Research Best Practice in Cyber-Resilient Systems

Dr Keith Joiner, Capability Systems Centre, School of Engineering and Information Technology (SEIT), University of New South Wales (UNSW) at Canberra, k.joiner@adfa.edu.au

Dr Elena Sitnikova, Australian Centre for Cyber Security, SEIT, UNSW at Canberra, e.sitnikova@adfa.edu.au

Dr Malcolm Tutty, Defence and Systems Institute, University of South Australia, maltuttyJAIME@hotmail.com

ABSTRACT

The rise in cyberspace threats and the importance of cybersecurity T&E has been well-documented, including from an Australian perspective where academics have recently lobbied the Australian Government for a more systemic response to the threat and the 2016 Australian Defence Whitepaper has begun that response. Consequently, there is a prospect of Australian Defence soon following the U.S. Defense lead and, with the assistance of U.S. Defense T&E agencies, conducting a series of selected cyber-survivability trials on major Australian Defence platforms, so as to kick-start cyber-survivability T&E at the Australian T&E agencies. Platforms to be evaluated are likely to include major ships, aircraft, land vehicles and joint command, control and communication systems. Australia sources its defence systems from different design houses in Europe and the U.S. and these come with different design vintages and differing extents to which their designs are Australianised. There is a real paucity of system design guidance on how to be resilient to the new cyber threats, especially across the breadth from micro-chips to whole systems like ships (i.e., "chip-to-ship"). These prospective Australian cyber-survivability trials are therefore an ideal opportunity to determine, compare and contrast how different cyber-resilient design features work at the sub-system, system and system-of-system level, in order to provide Defence and Australian industry with a list of best practices in cyber-resilient design requirements for future Australian defence systems. This paper recommends that if such trials proceed, they include a research element aimed at cataloguing best practice in cyber-resilient design, ideally with UNSW Canberra so those best practices focus cybersecurity teaching of Defence and Defence Industry students.

AUSTRALIAN DEFENCE CYBER-SURVIVABILITY T&E

The cyber threat to Australia has recently been documented by (Austin 2016) as part of an urgent call from the Australian Centre for Cyber Security (ACSC) for a more concerted and systemic approach by the Australian Government to its funding of academia and its departmental programs. As part of that same effort Joiner (2016) catalogued the significant operational benefits achieved in the U.S. Defense since cyber-security T&E was first made mandatory as part of its operational T&E in 2009, and he contrasted that with Australia's lack of cybersecurity test requirements in its Defence T&E policy. For example, he outlines the significant investment by the U.S. in the National Cyber Range (NCR) to underpin their cybersecurity T&E both developmentally and operationally (see also Brown et. al., 2015 and U.S. DoD, 2015). The new Australian (Defence Whitepaper 2016) has begun a more systemic response to cybersecurity by the Government (p. 51, pp. 85-86, p. 89, p. 121) with the associated (Defence Integrated Investment Program 2016) proposing significant investment in cyber-security training and test infrastructure (p. 27, p. 39, pp. 44-45, p. 117). Australia's Defence now needs to continue to follow the U.S. Defense by conducting cyber- survivability operational T&E on all major platforms and systems, so that it can be properly informed in the operational and technical risks of its current capabilities and the requirements for better cyber- resilience of its future capabilities. Joiner (2016) strongly recommended Australian Defence kick-start its capability for cyber-survivability T&E by asking U.S. Defense T&E agencies to help Australia conduct a select series of cyber-survivability trials on major Australian platforms and systems over the next few years.

If Australia's Defence agrees to cyber-survivability T&E policy and the kick-start trials, there is considerable scope to shape these trials to deliver findings beyond simply the cyber-resilience of each major platform and system trialed. Aspects that can be evaluated across the many sub-

systems, systems and systems-of-systems being collectively trialed, include where the system designs originated, their design vintage relative to information technologies and cyber threat development, and what, if any, cyber features provide unfortunate vulnerabilities or serendipitous resilience. Such a cross-section of findings concerning the cyber-resilience of Defence systems will help systems engineers with some benchmarks for specifying cyber-security requirements and in devolving these cyber-security requirements through system specification. The cyber threat has evolved so quickly, current Australian systems engineers are unlikely to be competent to adequately specify what system characteristics they need to give cyber-resilience, or even, what cyber-survivability test their systems need to pass. Some early best-practice evaluations have potential to dramatically improve the loquacity and effectiveness of today's systems engineers to set future system requirements and verification testing around these unfamiliar new threats.

CHARACTERISTICS OF AUSTRALIAN DEFENCE SYSTEMS

Parliamentary reports by Defence Materiel Organisation and the (Australian National Audit Office 2014) show that Australia purchases its Defence systems predominately from the U.S. or Europe with varying degrees of Australianisation. Increasingly those Defence systems that are sourced from the U.S. are either through U.S. Defense Foreign Military Sales (FMS) or purchased commercially from U.S. companies on the strength of their use by the U.S. military. Also, Australian Defence has sought to reduce the extent of Australianisation in order to realise less technical risk from such modifications. The alignment of Defence systems with the U.S. military varies somewhat by the environmental domain, with Australia's military aircraft and joint command, control and communication infrastructure achieving higher direct alignment with U.S. Defense systems than either maritime or land systems. Such observation does not mean there is not significant interoperability between all such defence systems used by Australia and its U.S. ally, simply that some domains have directly aligned to the same suppliers by buying common systems.

Common to all environmental domains is Australia's ingenuity in taking platforms that suite its geostrategic need for long ranges and platform autonomy, and combining these with the best surveillance and weapon systems. Recent examples include the Airborne Early Warning, Control and Surveillance aircraft, the Air Warfare Destroyer and the new Special Forces vehicle. Sometimes this ingenuity sees Australia integrate the best weapons from one country to the aging aircraft, ships or land vehicles of another country, such as the integration of the Advanced Short-Range Air-to-Air Missile to the Hornet aircraft, the MU-90 Lightweight torpedo to its Frigates, the Hellfire missile to its Armed Reconnaissance Helicopter, and at some future stage the Naval Strike Missile to the Joint Strike Fighter. Fundamental to this sovereign ingenuity is the ability to integrate, which now must include the need for comprehensive cyber-security and cyber-survivability T&E of integrated systems. Part of the success of such integrations has been procurement of platforms with standardised data-buses like Military Standard 1553 for aircraft.

Australia's off-the-shelf systems, such as the Abrahms Tanks (U.S.), C17 airlift aircraft (U.S.), Superhornet aircraft (U.S.) and the Landing Helicopter Dock ships (Spain), generally require some fitment of command, control and communications equipment to interoperate with the rest of Australia's forces. This is especially the case of any system that constitutes a network-centric warfare node, like the Landing Helicopter Dock ships that will carry tailorable force command nodes. Increasingly, such platforms carry electronic support measures that must be reprogrammed as threats evolve based on intelligence and counter-measure development. Such regular reprogramming constitutes an attack surface vector in its own right, sometimes outside the country-of-origin, and necessitating recheck of cyber-resilience. One of the engineering preferences of such spiral development is what is colloquially referred to as the '*grandfather principle*', where a system is only re-checked or requalified to its original standard. The rapidly evolving cyber threat is a challenge to these cost-limiting checks like the *grandfather principle*, because requalifying to a cyber-resilience standard of a few years ago, only risks every other interoperating system to a point of potential weakest link for cyber-attack. Such a concept of requalifying a reprogrammed system to evolving standards, when the system was purchased off-the-shelf in another country, is a particular challenge for Australia, since it undermines some of the principal cost-savings sought in choosing such an acquisition and support strategy in the first place.

The U.S. Defense is leading Western nations in the systematic conduct of cybersecurity T&E and therefore the universal understanding of cybersecurity risk and cyber-resilient design (Joiner 2015). Note the qualification in this statement is 'universally leading'. Adaptable European, Israeli and Asian

designers of Defence systems may have exemplary cyber-resilient designs in some areas of system design, especially those sub-systems of more recent design vintage. The Army's purchase, initial roll-out and upgrade of an Israeli battle-management system for its land forces is an example where such non-U.S. ingenuity for cyber-resilient design is being measured by Australian use. The combination of sourcing more Defence systems from the U.S. Defense stable and the U.S. rigour for cybersecurity T&E, ought to lead to a hypothesis that Australia will have a comparable level of cyber-resilience to that of the U.S, at least for that proportion of Defense systems purchased from the U.S. However, cyber threats and cyber-survivability are based, at the system-of-system level on the 'weakest link' available in a cyber-attack surface. Australia has a long history of australianising its foreign designs, as a minimum to interoperate with other legacy systems from Australia's mixed-stable of systems. So for example, a European-sourced refueling tanker aircraft must interoperate with the U.S.-sourced fighter aircraft that it refuels. Every Australianising modification and interoperation with a legacy Australian system potentially weakens the attack surface of the new system. Further, because Australian Defence is not conducting cyber-survivability as part of it operational T&E, there is simply no way of knowing how much such modifications and interoperations are weakening the cyber- resilience built and tested-in during the foreign certification.

The U.S. Defense, despite its overwhelming preference for home-grown Defense systems, also has the issues of mixed design vintage, legacy systems and some foreign-procured systems. Large scale exercises like the U.S. Army Modernization Brigade's Network Integration Experiment (NIE), deliberately look at the compatibility and cyber-resilience of the myriad of land systems through a part-experiment, part-operational exercise. The NIE has an annual battle rhythm to encourage spiral development and selective allied participation has begun to ensure U.S. forces can integrate with its key allies without weakening its cyber-resilience. Australia's current lack of cyber-survivability as part of its operational T&E risks the first known instances of cyber weakness being involvement in an allied exercise. Like a child with measles in a school ground, Australia could be asked to come back and play only once it gets better. The sad reality of cyber-defence though is that it largely has to be built-in and it is not something therefore that can be quickly remediated. To continue the analogy, early vaccination is far better than isolation and recovery care.

Australia also operates several types of Joint Task Forces (JTFs) consisting of the air, maritime, land and joint systems necessary to have a fused battlefield effect. (Tutty 2016) has characterised these JTFs as families-of-system-of-systems because of their ability to adapt and even evolve, particularly when combating an enemy threat over long periods of time where rotating forces are necessary. Much acquisition and operational effort has been expended in Western countries over the last decade to rapidly refit and requalify its counter-insurgency forces with the latest equipment and tactics to defeat cheap weaponry like improvised explosive devices. Future enemies, whether state or non-state, are likely to require future JTFs to adapt quickly to such force-protection vulnerabilities coupled with cyber-vulnerabilities. Characterising the cyber-survivability of Australia's future JTFs is problematic, since their configuration is based on the operational needs of the threat at the time and they are unique to Australia because of the mixed-acquisition sources. To some extent, ensuring contributing force elements all have good cyber-survivability (i.e., are vaccinated) does contribute to the overall JTF survivability, but the networked systems, as coupled and rapidly re-fitted and re-qualified as necessary, have unique attack surface and need some T&E of cyber-survivability ahead of any real use, if Australia is to have such JTFs fight and win. Only by developing cyber-representative threats in Australia's exercises with spiral development opportunities and regular battle-rhythms can such families-of-systems be confidently prepared for the cyber-threat they will face. Such exercise-level T&E of families-of-systems-of-systems is difficult to establish, at least until the network-centric warfare nodes used in these families undergo cyber-survivability T&E and build Australia's expertise and capacity for cyber-survivability T&E. The U.S. Defense capability to now undertake cyber-representative exercises with such families-of-systems-of-systems is testament that it is possible for Australia to get to this level provided it follows the U.S. lead, if not in scale, at least to equal rigour.

A selected list of suggested Defence systems to conduct cyber-survivability T&E on, as part of their operational T&E, is given in Table 1. This list includes a representative sample of European, U.S. and other suppliers, design vintages from around 1998 through to today, varying degrees of Australianisation, and importantly, at least two trials from each environmental domain, so that all the different U.S. Defense T&E agencies can pass their expertise to all the equivalent Australian Defence T&E agencies.

Domain	Project	When Likely	Why
Maritime	AWD	During Ship Qualification Trials near San Diego about 2019	Critical node C4ISR node, travels widely. Will operate with US. Has U.S.AEGIS but otherwise local derivation.
Maritime	LHD	2017	Critical C4ISR node, travels widely, operates with US. Is a non-U.S. case.
Maritime	ASMD	Around a RIMPAC	Critical defensive system. Will operate with US. Will inform cyber-resilience of follow-on designs in work (i.e., SEA 5000). Locally designed.
Land	LAND121 (Ph. 4) Hawkei	Final prototype T&E circa late 2016	Local design, first modern networked vehicle. Results inform L400 combat vehicle cyber-resilience
Land	JP2097	Vehicle OT&E mid-16, Network System OT&E in 2017	Critical offensive system with unique distributed attack surface topology. Operates with US. Has non-US vehicle, US equipment in network system.
Land	L200 BMS Tranche 2	Lead up to US NIE in May 17 as normal qualification (Q3 16)	Non-US. Critical C3 digital system. Will operate with US. NIE qualification shows U.S. process.
Land	L17/L19 Fire Coord'	Elements of L17 & L19 land fire systems that are digitized	Critical digital systems, partly U.S. derived but with local modifications to attack surfaces. Will operate with US.
Aero-space	JSF	Part of U.S. IOT&E program likely 2018. Repeat at AUS OT&E	Critical US-derived system, operates with US. Repeat CS T&E with AUS attack surface in 2019.
Aero-space	AEW&C	Around a U.S. based exercise 2017	Critical C4ISR node. Non-U.S. derived. Will be a surface to many other systems. Is operating with US.
Aero-space	KC30	Around a U.S. based exercise 2017, likely in concert with AEW&C	Critical system. Non-US derived. Is operating with US.
Joint	JP2008 Ph. 5 SATCOMM	Early de-risk OT&E for terminals in 2016. Later with NMS IOT&E in 2018	Critical C4ISR node. Supports allied operations in large region. Some COTS equipment of uncertain CS pedigree. NMS possible unique.
Joint	JORN Upgrade	IOT&E in 2019	Critical ISR feed. Supports allied ops in large region. Uncertain CS pedigree.
Joint	New hybrid civil/military ATC System	IOT&E in 2017	Software intensive. Critical feed to C4. COTS equipment of uncertain CS pedigrees.

Table 1: Suggested Cross-Section of Australian Defence Systems to do Cyber-Survivability Operational T&E.[i]

For readers unfamiliar with Defence acronyms and projects, a full list of the acronyms used in this table is included in the endnotes.

CYBER-RESILIENCY

Australia is increasingly dependent on cyber-systems and vulnerable to cyber-attacks resulting in potential national risk (Austin 2016). This dependency applies to digitally-enabled networks, military mission-critical systems and services; and requires a development of a strategic view on a possible cyber-resilient future within untrustworthy environments influenced both by technology and humans. In a military context, cyber resiliency is an ability of mission-critical systems to continue providing acceptable operations despite disruptions caused by cyber-attacks in a cyberspace.

In this main section we briefly explore ideas on evaluating cyber-resilient features at four different tier-levels of mission-critical military systems. These are related to: sub-system, system, system-of-system (SoS) and family-of-system-of-system (FoS) levels. In each case, the nature of the

vulnerability will be discussed and some initial concepts about testing strategies offered to indicate the nature of much needed operational test and evaluation (OT&E) and research.

Cyber-warfare literature highlights and reiterates the complex role of humans in cyber-physical systems, such as the concept of the Cyber-Physical-Human World (MITRE) and three-dimensional spectrum of threats: software, hardware and people (DSTO) However, in this paper the research proposed would only describe cyber-resilient features relating to first two categories: hardware-based (HW Trojans, counterfeit electronic parts) and software-based (viruses, worms, spyware, exploits and protocols exploits).

EVALUATING CYBER-RESILENT FEATURES AT THE SUB-SYSTEM LEVEL

Sub-system cyber-resilience is generally achieved through a small number of suppliers and the advantages of relatively controllable laboratory testing. However, due to a broad spectrum of system functionalities and increasing complexity of mission critical systems, supplier-chains are growing, increasing the potential vulnerabilities within a variety of sub-systems, including software-intensive systems that are potential targets to cyber-attacks.

Cyber-attacks on sub-system level may include hardware Trojans that are malicious and designed to compromise systems that contain electronic circuits by intentionally modifying these. These might be introduced when adding new chips or modifying existing circuits and introducing new physical process and logic functions. According to CNN, counterfeit electronic sub-system parts have been incorporated to the critical U.S. military systems by a sub-contractor company from China, thus putting helicopters and surveillance systems at risk, (Courson 2011).

The Lockheed Martin F-35 Joint Strike Fighter is one of the complex mission critical systems, often referred to as a “flying computer”. Its software controls aircraft functions and consists of 8.5 millions of lines of code (Australian Senate 2016). The Automatic Logistic Information System (ALIS) is one of the sub-systems integrated within the aircraft that could make the aircraft vulnerable to cyber-attacks (U.S. DoD 2016, p. 38 & p. 78). Chinese military hackers have penetrated major unclassified defence sub-contractor systems causing leak of information about the air fighter (revealed by NSA). Last year JSF program executive officer Lt. Gen. Bogan admitted that ALIS software is “way behind”. During aircraft maintenance the ALIS sub-system proved incapable of handling the download of large data files to laptops via a commercial WiFi network. This is a potential vulnerability for the system while it cannot deal with the big data. Maintenance teams found 80% cases where the ALIS is “false positive” - indicated broken parts while they were not. JPO spokesmen Joe DellaVedova highlighted “…robust cyber vulnerability testing is essential”, (Malenic 2016).

Air Warfare Destroyer (AWD) is complex mission-critical system developing in Australia. It integrates sub-systems such as an integrated platform management system (IPMS) and an AEGIS radar system along with other sub-systems within the ship. IPMS is a distributed architecture system that is used on the ship for the real-time monitoring and control mechanical, electrical machinery and systems (power generation and distribution, heating, temperature and ventilation control and fire emergency). These systems are controlled by distributed automated process control and SCADA systems that could be vulnerable to cyber-attacks. In 2010 a sophisticated malware Stuxnet was found in a nuclear plant taking over and re-programming PLCs. It later spread to other plants. Similar to any other industry sectors, SCADA systems in defence sector, for example in the AWD IPMS, are potentially vulnerable to commonly known Database and SQL injections. Databases used by control systems are often connected to databases or computers with web-enabled applications located on the business network. Most use Structured Query Language (SQL), and many will have web interfaces that may be vulnerable to web attacks like SQL injection. Thus such databases are attractive to hackers who can exploit the communications channel between the two networks and bypass the security mechanisms.

AEGIS is designed and developed as a naval system integrating radar and missile systems. This sub-system is heavily dependent on GPS navigation and timing, remote sensing, automatic control and surveillance. GPS plays a key role on Destroyer positioning and is vital for accuracy in targeting the missile defence systems. Experts predict if the timing source that allows mission critical system communicate is attacked, the system can be made to fail. Experiments can imitate hackers conducting a “spoofing attack”, where they produce and broadcast a falsified version of GPS signal without causing the GPS receiver to alarm on the false signal. With several years delay already within the

AWD program, one of the major issues of the operational suitability of this ship is likely to be the potential cyber-vulnerability of its legacy systems. In the past process control systems were designed without security in mind, but now their integration requires cyber-resiliency testing.

For each Defence cyber-survivability trial proposed in Table 1, the type of information sought on each of the sub-systems of that major platform or system should include those indicative items at Table 2.

Domain/layer	Cyber-survivability trial
Hardware /firmware	General and specialised processors Embedded firmware Circuits and chips
Software	Software on sub-system components: applications, services, DBM
Operating system	General –purpose OS, Real-time OS (RTOS)
Networking / communication	Communicating Protocols Networking configurations
Information databases	Databases, knowledge bases, big data

Table 2. Sub-system level: Cyber-survivability trial for vulnerable features

EVALUATING CYBER-RESILIENT FEATURES AT THE SYSTEM LEVEL

System cyber-resilience is generally achieved through the systems engineering control of a major design house over a number of sub-system suppliers working towards overall sell-off to a foreign or Australian Defence regulator and project office. Testing for cyber-resilience is usually achieved as part of complete system verification of functional requirements, performing vulnerability assessment and penetration testing of completed systems like that outlined by U.S. DoD (Brown, et. al., 2015).

Vulnerabilities to malicious elements are ubiquitous in complex systems. Information collected by hackers through intrusion into the system can be used for future attacks. For example, invasion into sub-contractor's networks by Chinese hacker group compromised The NY Times and other organisations' networks including defence contractors. Aumlib and Ixeshe malware has been inserted. According to FireEye, Aumlib encodes certain HTTP communications and a new version of Ixeshe uses new network traffic patterns, possibly to evade traditional network security systems and use compromised servers housed inside targeted organisations such as command-and-control (C&C) servers, (Lennon 2013).

Protocol exploitations are common vulnerabilities at the systems level. Standard protocols are used in systems control environments. They are OPC Data Access 3.0, OPC Alarms, OPC Data Exchange, and OPC Data-XML. These standards and application programming interfaces are supported and used in Windows XP and Windows Server additions (MITRE 2015). Security implications and vulnerabilities range from simple system enumeration and password vulnerabilities to more complex remote-registry tampering and buffer-overflow flaws. These vulnerabilities bring risks of installing undetected malware, denial-of-service attacks, host-escalation privileges and even calculated shutdown due to an overload flaw.

To bypass firewalls or system intrusion detection system (IDS) and stay in a network unnoticed, hackers are using commonly used ports TCP:80 (HTTP), TCP:443 (HTTPS), TCP:25 (SMTP) and TCP/UDP:53 (DNS). For internal connections common ports are TCP/UDP:135 (RPC), TCP/UDP:22 (SSH), and TCP/UDP:3389 (RDP).

Data that flows within system networks between servers, databases, and control devices can be compromised in different scenarios: (1) hacker re-routes data that is in transit on a network, (2) capture and analyse critical data traffic, and (3) reverse engineer control protocols and gain command over control communications. By combining these scenarios, a hacker can be a "Man-in-the-Middle" and can control the data flowing in a network, and direct both real and "spoofed" traffic to network resources in support of the desired malicious outcome.

For each Defence cyber-survivability trial the type of information sought on the systems of each major

platform or system should include those indicative items at Table 3.

Domain/layer	Cyber-survivability trial
System /network component	Firewalls, servers, layered architecture
Mobile system/network component	Laptops, smart devices
Software	Software on sub-system components: applications, services, DBM
Operating system	General –purpose OS, Real-time OS (RTOS)
Networking / communication	Communicating Protocols Networking configurations
Information stores	Databases, knowledge bases, big data
Cloud, virtualisation, middleware infrastructure	VMM, service-oriented infrastructure, shared services
Mission function Application service	Mission applications

Table 3. System level: Cyber-survivability trial for vulnerable features

At the system-level, the proposed cyber-survivability trials also represent an opportunity to research a broad cross-section of Defence system for their most effective cyber defensive strategies, and therein, what system features aid such defensive resilience. The MITRE Corporation has developed an Adversarial Tactics Techniques and Common Knowledge (ATT&CK) framework for modelling and mapping post-exploit actions of an advanced persistent threat (APT). It currently has 95 different APTs mapped to 9 categories (MITRE 2015). For example, for the Command and Control *category* APT includes: commonly/uncommonly used port, custom layer application protocol, data obfuscation, standard app/non-app layer protocol, standard/custom encryption cipher, peer connections. For privilege escalation category: Bypass UAC, DLL injection and exploitation of vulnerability. Further, MITRE has also developed a method – time anomaly detection, principally for protecting GPS Receivers against spoofing attacks (MITRE 2014).

EVALUATING CYBER-RESILIENT FEATURES AT THE SYSTEM-OF-SYSTEM LEVEL

System-of-system (SoS) cyber-resilience is generally achieved through the cyber-resilience of the individual systems coupled with the operational oversight of an operational manager and their cyber-monitoring capability. In Australia only networked Defence information systems are currently known to be the subject of continuous cyber monitoring. The majority of Defence SoS like fighter aircraft, artillery and combat ships have no cyber-intrusion monitoring or even a handbook of operational characteristics symptomatic of cyber intrusion or attack and how to minimise the impact.

The classic design technique for reliability of SoSs has been to incorporate redundancy, however, cyber threats are particularly viral; in that, if they can penetrate one system, they will most likely penetrate the identical redundant systems. Cybersecurity experts have a relatively new term to describe the degradation of a system to cyber-attack called ‘degeneracy’, where systems that perform the same critical function but in different ways give resilience to how a system performs when under cyber-attack (Ormrod 2015). Testing for cyber-resilience is usually achieved only by the operator as part of complete system validation, meaning the work-arounds require costly monitoring, training and other operational techniques until remediation can be implemented, hopefully as part of scheduled system- level spiral developments. Defence is only now coming to grip with this as elements work to incorporate T&E of their increasingly networked information systems into the ‘mission systems’ designed for operational usage.

The proposed cyber-survivability trials at Table 1 each represent a system-of-system and each will be somewhat unique, such that it will be a limited dataset at this higher level from which to look for meta-lessons. Notwithstanding this limitation, the types of measures that might be used to compare cyber-resilience of these unique systems-of-systems could be:

- The number and type of like (but not identical) systems where degeneracy occurs.
- The number of systems-of-systems that can successfully use what types of cyber-operationally defensive measures.
- How resource-intensive are the cyber-operationally defensive measures to employ on each system-of-system.
- The actual time to render each system-of-system ineffective using different types of cyber-threat (Note to de-classify this, may need to use time relative to each other or some arbitrary benchmark).
- The types of operationally visible symptoms of cyber-attack and how to distinguish these from other types of malfunction or operational response.

EVALUATING CYBER-RESILIENT FEATURES AT THE FAMILY-OF-SYSTEM-OF-SYSTEM LEVEL

The proposed early Australian cyber-survivability trials are not at the level of a JTF or family- of-SoSs (or FoS) level, although the cyber-resilience of the system-of-system, such as ship or aircraft, can be used to hypothesis what vulnerabilities these SoSs might introduce to future JTFs that incorporate them. For those systems-of-systems that are network-centric warfare nodes critical to particular types of JTF, such as the LHD ship to an Amphibious JTF or AEW&C aircraft to the air control of a Strike JTF, then significant extrapolations of effects at this higher-level could be made.

New research into SoS applications for military capabilities recognise that there are some common attributes across the traditional subsystem, system and SoS continuum. (Tutty 2016) argues that most SoS's need to be explicitly treated as Families of SoS (FoS) when military forces are operating as Joint Task Forces and/or during major training or evaluation exercises. Given that many of our military capabilities are primarily about the application of fires, as shown at Figure 1 for a typical joint fires targeting cycle, any structuring of Defence cyber survivability and reliance needs to be cognizant of many military capability truisms and where such research can be optimised to military outcomes

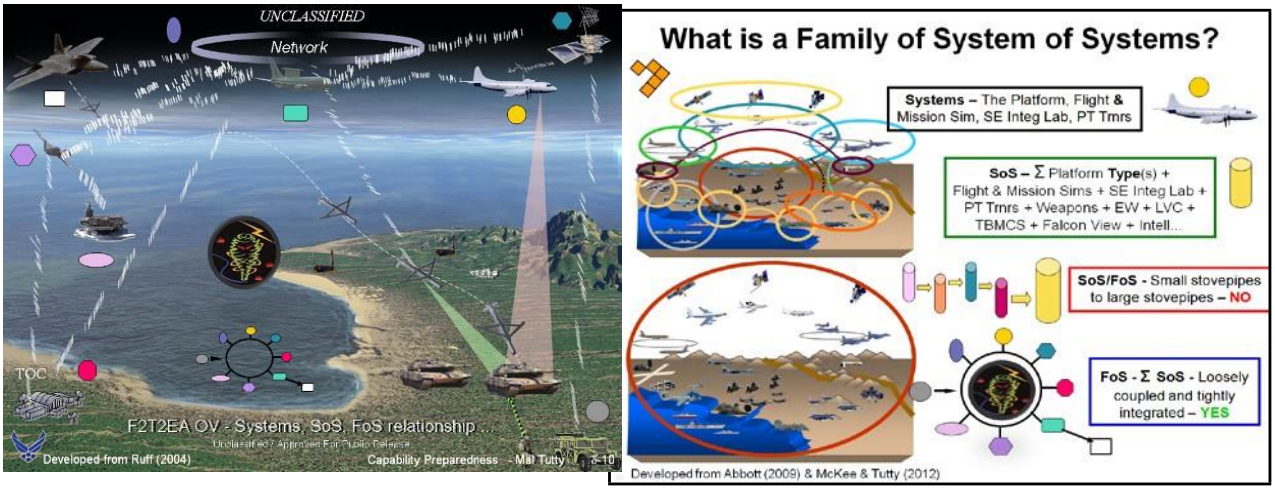


Figure 1: Typical joint fires kinetic warfare application and the SoS, and family of SoS (FoS) construct, Tutty (2016)

The work by (Tutty 2016) proposes that in order to bring the necessary operational confidence to a FoS, at least within a military JTF context, the current systems development and T&E process needs to be fundamentally altered and extended to include persistent (i.e. spiral) experiment, test and evaluation (ET&E) at the FoS level, with a narrowed focus of essential operational effects that must be achieved and essentially undesirable effects that must not occur (NATO ALWI-2 2004). The use by Tutty (2016) of the term 'experiment' with 'T&E' is deliberate to indicate that at the FoS-level, testing all permutations are not possible without combining rigorous modelling and simulation that fuses what is achievable in what is known as a live, virtual and constructive (LVC) test environment. Large-scale LVC FoS-level military experimentation exercises are becoming an increasing feature of the U.S. military calendar (i.e. Exercises BOLD QUEST, TALISMAN SABRE and NIE). These ET&E events

do include a cyber-survivability element whereby all candidate systems-of-systems go through a qualification process which is repeated each year in recognition that the systems-of-systems have evolved and so too have the threats. Some laboratory testing in that annual battle-rhythm to the ET&E establishes high-threat, high-vulnerability behaviours, so that at the FoS-level some experimental control can infuse and defuse FoS-level effects to ensure everyone benefits. For example, some effects of high-end cyber threats might be introduced without real release so as to prevent contagion. Such FoS-level ET&E has to reduce the level of what can be evaluated to an essential subset of what must be achieved and what must not happen, because the complexity, adaptability and human involvement in an military JTF FoS would collect too much data with insufficient repetition to otherwise complete analyse before the next annual event. For (McKee and Tutty 2014) this focus of ET&E at the FoS-level should necessarily be into weapon effects, electromagnetic effects and collateral damage, as those things that can both intentionally or undesirably kill. A schematic showing the inputs to an ET&E within fused LVC environments is shown in Figure 2 (McKee & Tutty 2014).

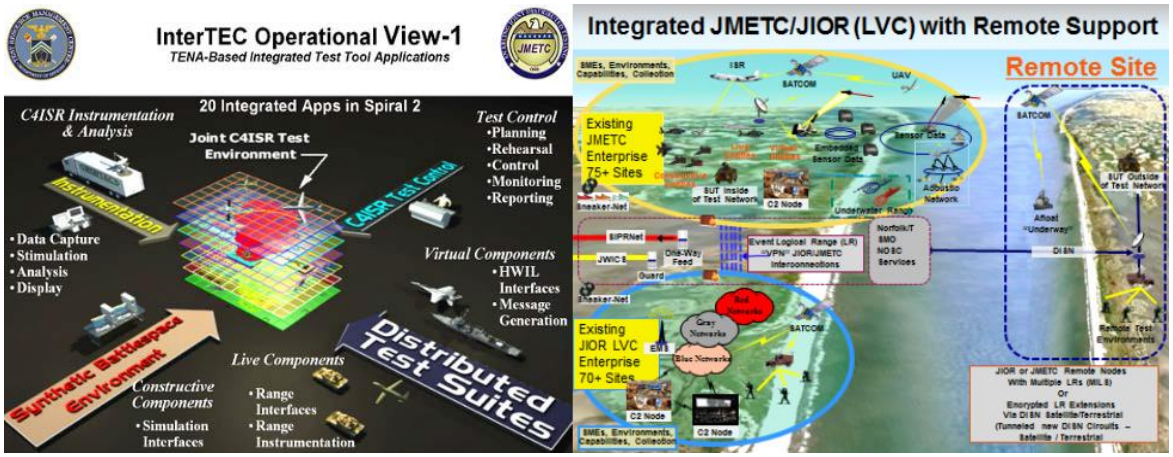


Figure 2: US Distributed M&S LVC operational view via InterTEC and the 'One Approach' for joint fires, Counter IED and cyber warfare of (McKee and Tutty 2014)

To implement this strategy, a change in focus by both the systems engineering and the experimentation and T&E organisations will be needed, so that they are able to also conduct scientifically rigorous testing, training, and experimentation that build confidence and removes risks in capabilities for conducting secure, network-enabled real-time kinetic and non-kinetic effects. This concept is shown diagrammatically at Figure 2 with operational views via InterTEC and, more importantly, a joining together of the test, training kinetic and non-kinetic EW and cyber worlds at right.

The ability to independently test systems, SoS, and FoS using a scientifically defensible approach using the LVC environment is critical. Rarely can nations successfully get all the entities necessary to accomplish representative experimentation nationally, let alone across a Coalition, to investigate the confidence in such operational scenarios during exercises, training and test/experimentation activities. The LVC needs to provide the mechanism to insert new subsystems and systems into virtual and constructive systems after enough M&S has confirmed basic form and fit criteria have been met and that functional criteria are suitable (see for example referenced military handbook (MIL-HDBK-1763 1998) and the NATO (JAIME CODEx 2014)). (Tutty et. al. 2016) proposes a new view of how the confidence in cyber operations can be shown to be more operationally useful to future operational commanders in deciding how to achieve their required operational effect and whether to use kinetic weapons or non-kinetic electronic or cyber warfare options.

The proposed cyber-survivability trials at Table 1 are not at the FoS-level, but how cyber-resilient the ones that are network-centric nodes in a military JTF are, can inform how future Australian JTF might perform at that level. Such operational extrapolation (hypotheses) is likely to inform the importance of Australia developing its own annual ET&E events or synchronising and participating in the necessary allied ones, especially where Australia is yet to manifest operationally representative cyber-threats suitable for competent and confident use at such scale. At least part of the research across the proposed trials should be into such extrapolation and hypotheses concerning the FoS-level performance

involving the systems-of-systems tested.

EFFECTIVE COORDINATION OF EVALUATION ON EACH TRIAL AND RESEARCH ACROSS TRIALS

Data collection and analysis at multiple systems levels, across the breadth of cyber-survivability trials proposed will be difficult. Australian T&E agencies will need to avoid extraneous cross-trial tasks during any such operational trials, so as to be free to learn the test techniques and coordination from the assisting U.S. T&E agencies and to report to the applicable Service Chief what operational risks and remediations should be applied to the specific system-of-system they are evaluating. A research centre like the Australian Centre for Cyber Security (ACCS), with support from Defence Science and Technology, should be engaged to agree the cross-trial analysis data on cyber-resilience, analyse that data and report the best-practice cyber-resilient design practices for future Defence systems development in Australia. Some examples of such cross-trial data requirements have been suggested here and the types of benefits hypothesised. If these proposed trials are more fully scoped, the ACCS should be tasked and funded to finalise cross-trial data requirements, analyse and report best practices.

BENEFITS OF DOCUMENTING BEST-PRACTICE CYBER-RESILIENCE IN SYSTEMS DESIGN

Having research into best-practice cyber-resilience in systems design as part of the proposed kick-start cyber-survivability trials should realise the following summary benefits:

- Greater traceability in each trial between any cyber vulnerabilities or cyber-resilience exhibited and the underpinning likely causes in the design.
- A better basis to explain to operational staffs who are training to defend legacy platforms and systems about why the designs they have the resilience and vulnerabilities characteristics.
- Greater awareness by Defence capability planners on how to progress design requirements for future systems.
- A guide for systems engineers in Defence and Defence Industry on the pointers and pitfalls in developing detailed specification requirements for design of future systems.
- A design-focused basis to better focus future cyber-survivability testing on the likely vulnerabilities sooner in a test program.
- A sound and cost-effective basis from which to prioritise what other legacy Defence systems-of- systems should undergo operational cyber-survivability T&E.
- A basis to estimate what military JTF at the FoS-level may be more vulnerable or resilient than others for a high cyber-threat environment.
- Indicative guidance on the cyber-resilience of common supply and design sources for Defence systems at the sub-system, system and system-of-system levels.
- High-level guidance on prioritising what, if any, systems-of-systems may need early upgrade or retirement in order to cope with the cyber-threat posed by potential adversaries exploiting the Information Age, and what design features are driving that upgrade or retirement.
- A great research basis to inform cybersecurity education for students from Defence, Defence Industry and other Government departments.

CONCLUSIONS

In response to rising cyberspace threats and the Australian (Defence Whitepaper 2016) there is a prospect of Australian Defence soon following the U.S. Defense lead and, with the assistance of U.S. Defense T&E agencies, conducting a series of selected cyber-survivability trials on major Australian Defence platforms, so as to kick-start cyber- survivability T&E at the Australian T&E agencies. Platforms to be evaluated are likely to include major ships, aircraft, land vehicles and

joint command, control and communication systems. This paper has proposed a cross-section of Defence platforms and systems in which to kick-start cyber-survivability operational T&E. Further, the authors recommend underpinning such kick-start trials with some Australian-led research on what is best-practice cyber-resilient design and sourcing at the sub-system, system and system-of-system level. The proposed cross-trial research would provide much needed system design guidance on how to be resilient to the new cyber threats, especially across the breadth from micro-chips to whole systems like ships (i.e., "chip-to-ship"). The authors have given indicative areas in which to catalogue system design during the trials and compare with the cyber-survivability performance achieved. They have also proposed some research extrapolation (hypotheses) of trial results to the military JTF FoS-level in order to see what might be the criticalities of such JTF in a high cyber-threat environment and what experiment, test and evaluation may be necessary for Australia at the National and allied force-level. Numerous benefits of such under-pinning research for these Defence trials are listed, but the primary motive of such research for the Australian Center for Cybersecurity is better, researched-informed teaching of its students in cybersecurity.

REFERENCES

AAP-6, 2010, *NATO Glossary of Terms and Definitions* (English and French), NATO Military Standardization Agency, [NATO Standardization Office as of July 2014], 29 April 2014

Alberts, Dr D.S., and Hayes Dr R.E., 2002, *Experimentation; Code of Best Practice*, Command and Control Research Program, [Online, accessed 1 September 2006], http://www.dodccrp.org

Alberts, Dr D.S., and Hayes, Dr R.E., 2007, *Planning: Complex Endeavours*. Command and Control Research Program, April 2007 [Online, accessed 15 July 2007]. http://www.dodccrp.org

ALWI-2, 2004, *Final Report, Follow-up Study, Aircraft, Launcher & Weapon Interoperability (ALWI-2)*, NATO Air Force Armaments Group (NAFAG), Air Group 2 on Air Weapons, NATO Industrial Advisory Group (NIAG), AC/224(AG/2)D(2004)0001, 7 April 2004.

Austin, G., "*Australia Rearmed! Future Needs for Cyber-Enabled Warfare*", Discussion Paper No 1 of the Australian Centre for Cyber Security at University of New South Wales, Canberra, developed from the International Conference '*Redefining R&D Needs for Australian Cyber Security*' on 16 November 2015 and released publically on 19 January 2016. Available at https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/news/australia-rearmed.

Australian Defence White Paper, 2016, '*2016 Defence Integrated Investment Program*', available from www.defence.gov.au.

Australian Senate (2016), *Proceedings of Senate Inquiry into F35 Aircraft Acquisition held on 22 March in Canberra*. Testimony by Mr Jeff Babione, Executive Vice-President and General Manager of F35 Lightning II Programm, Lockheed Martin.

Brown, C.; Christensen, P.; McNeil, J. & Messerschmidt, L., 2015, Using the Developmental Evaluation Framework to Right Size Cyber T&E Test Data and Infrastructure Requirements. *The ITEA Journal*; 36: pp. 26-34.

Christensen, P., 2007, *Information Operations and the NetReady Key Performance Parameter in US DoD Systems Acquisition & T&E*, Invited Paper Information, Decision and Control IDC Conference 2007, Adelaide, South Australia February 2007.

Courson P., 2011, CNNReport: Bogus U.S. Military parts Traced to China http://edition.cnn.com/2011/11/07/us/u-s-military-bogus-parts/ CNN.

Defence Materiel Organisation and Australian National Audit Office. 2014, Report No. 14 2014-15: 2013-14 Major Projects Report. Canberra: ANAO.

Department of Defense (U.S.), 2016, Director of Operational Test and Evaluation Annual Report to Congress for 2015 for the F35 Aircraft. Available at http://www.dote.osd.mil/pub/reports/FY2015/pdf/dod/2015f35jsf.pdf.

Department of Defense (U.S.) (2015). NCR Overview. Accessed at www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

DSTO, 2016, *Future Cyber Security Landscape: A Perspective on the Future*, viewed 3 Feb 2016 http://www.dsto.defence.gov.au/publication/future-cyber-security-landscape-perspective-future

Garstka, J.J., 2000, *Network Centric Warfare: An Overview of Emerging Theory*, Directorate for C4 Systems, US DoD, Washington, USA [Online, accessed 10 May 2004]. http://www.mors.org/publications/phalanx/dec00/feature.htm

GUIDEx, 2006, *TTCP Guide for Understanding and Implementing Defense Experimentation (GUIDEx)*, The Technical Cooperation Program, [Online, accessed 15 July 2007]. www.dtic.mil/ttcp/guidex.htm

Joiner, K. F., 2016, "*Integrating Cyber-Survivability into Future ADF Platform Development*", Discussion Paper No 2 of the Australian Centre for Cyber Security at University of New South Wales, Canberra, developed from the International Conference '*Redefining R&D Needs for Australian Cyber Security*' on 16 November 2015 and publically released on 19 January 2016. Available at https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/news/cyber-survivability.

Lennon M, 2013, Attackers Upgrade Aumlib and Ixeshe malware Used against New York Times., viewed 3 Feb 2016 http://www.securityweek.com/attackers-upgrade-aumlib-and-ixeshe-malware-used-against-new-york-times

Malenic M., 2016, C4iSR: Air DoD chief tester warns on F-35 cyber, software issues Washington, DC - IHS Jane's Defence Weekly, Jan 2016)

McKee S.V., & Tutty, M.G., 2012, Doing more of the right high-end effects-based things without more - from Basics to Families of System of Systems Capabilities, *ITEA Journal, September 2012,* JITE-33-03-05 pp 203 - 243 [Posted online September 2012] at www.maltutty.com / Contents

MIL-HDBK-1763, 1998, *Aircraft Stores Compatibility: Systems Engineering Data Requirements and Test Procedures*, US Department of Defence Handbook, Revision 15 June 1998, USA.

MITRE, Thinking Forward Archives, viewed 3 Feb 2016, http://www.mitre.org/capabilities/cybersecurity/overview/thinking-forward/thinking-forward-archives-0

MITRE, 2014, Time Anomaly Detection Applique (TADA), viewed 3 Feb 2016 http://www.mitre.org/research/technology-transfer/technology-licensing/time-anomaly-detection-appliqu%C3%A9-tada

MITRE, 2015, An Overview of MITRE Cyber Situational Awareness Solutions, viewed 3 Feb 2015, http://www.mitre.org/publications/technical-papers/an-overview-of-mitre-cyber-situational-awareness-solutions

NATO JAIME CODEx, 2014, *Armament Systems Compatibility*: *Joint fires Armament Integrated Mission Environment, Armament Systems Compatibility: Code of Practice for Test, Experimentation and Certification – JAIME CODEx and The Tests*, Disclosure Draft V2.0, [Posted online October 2014] www.maltutty.com

Ormrod, D., "Toward a Military Cyber Maturity Model", Proceedings of the International Conference '*Redefining R&D Needs for Australian Cyber Security*', 16 November 2015.

Stallard, C.T., 2009, *Integrating the non-kinetic rope into the fabric of operational planning*, Air Command and Staff College, Air University, USAF, Maxwell AFB, Alabama

Tutty, M.G., and McKee, S., 2014, Keeping Test and Experimentation simple and operationally focused in a Complex World, *Systems Engineering and T&E, SETE Symposium 2014*, Adelaide South Australia, 28 – 30 April 2014 [Paper and Presentation posted online April 2014] www.maltutty.com / Contents

Tutty, M.G., 2015, The Profession of Arms in the Information Age, *Systems Engineering and T&E Symposium 2015*, Canberra, ACT, Australia, 27 – 29 April 2015

Tutty, M.G., 2016, *The profession of arms in the information age: operational joint fires capability preparedness in a small-world*, Dissertation with University of South Australia, 1 January 2016, [Posted online 10 January 2016] www.maltutty.com / Contents

Tutty, M.G., McKee, S.V. and Sitnikova, E., 2016, Towards Joint fires superiority: kinetic and non-kinetic electronic and cyber warfare operations, *SETE Symposium 2016*, Melbourne, Victoria,

BIOGRAPHIES

Dr Keith Joiner, CSC, joined the Air Force in 1985 and became an aeronautical engineer, project manager and teacher over a 30-year career before joining the University of New South Wales in 2015 as a senior lecturer in test and evaluation. From 2010 to 2014 he was the Director-General of Test and Evaluation for the Australian Defence Force, where he was awarded a Conspicuous Service Cross. He is a Certified Practising Engineer and a Certified Practising Project Director.

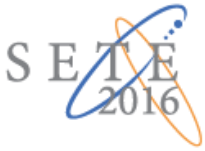
Dr Elena Sitnikova PhD, BE (Hons), CSSLP is an experienced researcher and academic within the Australian Centre for Cyber Security (ACCS) at the University of NSW. Her main research interests are in critical infrastructure protection and cyber security, quality assurance and enterprise process capability improvement. Elena currently leads the Critical Infrastructure area, carrying out research projects in cyber security in SCADA and process control systems with industry, State and Federal Government partners in Australia.

Dr Malcolm Tutty has served in the Air Force, Public Service and Industry in a multitude of test, operations, engineering, staff, project management and command roles. This includes being a flight test armament engineer at the Aircraft Research & Development Unit, an aircraft stores compatibility engineer while on exchange with the USAF during Gulf War I, a director of the Woomera Test Range and launch authority for two hypersonic firings into space. Recently he deployed during Operation SLIPPER into Afghanistan to conduct coalition interoperability trials and field several new advanced EW systems. He has been a Fellow of both the Royal Aeronautical Society and the Institution of Engineers (Australia) for over a decade.

---

[i] Defence acronyms and terms not explained elsewhere in this paper are as follows alphabetically:
AEGIS – U.S designed air warning radar.
AEW&C – Airborne Early Warning & Control Aircraft
ASC – armament systems compatibility
ASCENG – Aircraft Stores Compatibility Engineering
ASMD – Anti-Ship Missile Defence
ATC – Air Traffic Control (Radar)
AWD – Air Warfare Destroyer
BMS – Battle-Management System
COTS – Commercial Off-The-Shelf
CS – Cyber-Survivability
EMS – Electro-Magnetic Spectrum
Fires – i. The effects of lethal or non-lethal weapons. NATO AAP 6 (2010)
ii. the use of ***weapon systems*** to create a specific lethal or nonlethal effect on a target.
All fires are normally synchronized and integrated to achieve synergistic results.
Fires can be delivered by air, land, maritime, or special operations forces.
As agreed by the Fives Eyes in US JP 3-09 (2006) and FM 3-09.32 (2010)
Hawkei – Australian-designed light tactical protected vehicle
IED – Improvised Explosive Devices
IA – Information Assurance
IO – Information Operations
IOC – Initial Operational Capability
IOT&E – Initial OT&E
ISR – Intelligence Surveillance & Reconnaissance
JAIME – Joint fires Armament Integrated Mission Environment
Joint Fires – Fires applied during the employment of forces from two or more components, in coordinated action toward a common objective.
JP2008 – Joint project for new satellite communication family of systems
JP2097 – Joint project for new Special Forces ground mobile patrol capability
JSF – F-35 Joint Strike Fighter aircraft
KC30 – Australian multi-role tanker refueling aircraft
Land 17/19 – Two land projects that collectively digitize elements of artillery & other joint fire weapons
Land 154 – An omnibus project to protect Australian military and civilian personnel from remote control

electronic warfare IEDs
Land 200 – An omnibus land project to digitize much of Australian Army's forces
Land 400 – Large land project for protected offensive mobile capabilities for a defended objective. Initially replaces amphibious light armoured vehicles.
LHD – Landing Helicopter Deck ship
LVC – Live, virtual and constructive
NIE – U.S. Network Integration Exercise
NEO – Network-enabled operations
NMS – Network Management System
OT&E – Operational T&E
Q3 – Quarter 3 (of a calendar year)
SATCOMM – Satellite Communications
SEA5000 – Maritime project for replacement frigates.


S E T E
2016